1. A communication device operable in a domain-based digital rights management environment, comprising:

a processing element;

a receiver, coupled to and controlled by the processing element, operable to receive incoming messages to the communication device;

a transmitter, coupled to and controlled by the processing element, operable to transmit output messages of the communication device; and

a digital rights management module coupled to the processing element that controls operation of the communication device within the domain-based digital rights management environment;

wherein the digital rights management module of the communication device in combination with a domain authority of the domain-based digital rights management environment is operable to selectively add the communication device to a domain having one or more communication devices that share a cryptographic key and thus permit the communication device to selectively receive and decrypt digital content based upon membership in the domain.

2. The communication device of claim 1, wherein the transmitter is a limited range transmitter having a limited communication range and operable to transit the digital content to a trusted communication device within the limited communication range.

3. The communication device of claim 1, wherein in response to receiving a user request, the digital rights management module causes the transmitter of the communication device to transmit to a domain authority a request to register the communication device into the domain; and

wherein if the communication device is determined to have access to one or more valid cryptographic elements, the digital rights management module causes the receiver of the communication device to receive over a communications channel the cryptographic key of the domain from the domain authority to link the communication device to the domain.

4. The communication device of claim 3, wherein the digital rights management module in combination with the domain authority removes the communication device from the domain, comprising:

in response to the request of the user of the domain to remove the communication device, the digital rights management module of the communication device causes the transmitter to transmit a request that the communication device be removed from the domain;

in response to the request that the communication device be removed from the domain, the communication device receives from the domain authority via the secure communications channel a command to remove the cryptographic key of the domain from the communication device; and

upon receiving the command from the domain authority, the digital rights management module of the communication device removes the cryptographic key of the domain.

5. The communication device of claim 1, wherein in response to the digital rights management module of the communication device causing the transmitter to transmit a request for digital content, at least one of the digital rights management module of the communication device and the domain authority verifies authenticity of the domain; and

wherein upon verification of the authenticity of the domain, the receiver of the communication device receives an encrypted form of the requested digital content that is bound to the cryptographic key of the domain in which the communication device is registered.

6. The communication device of claim 1, wherein the digital rights management module of the communication device enforces usage rules associated with the requested digital content and received by the receiver in a content package containing the requested digital content.

7. The communication device of claim 6, wherein the content package comprises a binary representation rights table that contains the usage rules.

8. The communication device of claim 7, wherein the binary representation rights table comprises a plurality of sections having predefined tokens.

9. The communication device of claim 1, wherein the digital rights management module, in response to the transmitter of the communication device receiving a request from a second communication device of the domain requesting the digital content, causes the transmitter to transmit the requested digital content from a storage element to the second communication device.

10. The communication device of claim 1, wherein in response to a request of the user of the communication device, the digital rights management module causes the transmitter to transmit a request for digital content that is not available in the domain; and

wherein after authenticity of the domain has been verified, the receiver receives an encrypted form of the requested digital content that is bound to the cryptographic key of the domain to which the communication device is registered.

11. The communication device of claim 10, wherein the encrypted form of the requested digital content is contained in a content package.

12. The communication device of claim 11, wherein the content package further comprises a binary representation rights table that contains the usage rules of the requested digital content.

13. The communication device of claim 12, wherein the binary representation rights table comprises a plurality of sections having predefined tokens.

14. The communication device of claim 10, wherein the digital rights management module of the communication device stores the encrypted digital content in an open-access storage element.

15. The communication device of claim 10, wherein the digital rights management module of the communication device enforces usage rules associated with the requested digital content and received by the receiver in a content package containing the requested digital content.

16. The communication device of claim 15, wherein the content package comprises a binary representation rights table that contains the usage rules.

17. The communication device of claim 16, wherein the binary representation rights table comprises a plurality of sections having predefined tokens.

18. The communication device of claim 1, wherein in response to the receiver receiving a request from a second communication device of the one or more communication devices of the domain for the digital content and the digital rights management module verifying the authenticity of the second communication device, the digital rights management module causing the transmitter to transmit

the requested digital content from a storage element of the communication device to the second communication device.

19. The communication device of claim 1, wherein the digital rights management module causes digital legacy content received from a source external to the domain to be stored in a storage element of the communication device; and

wherein in response to a request from a second communication device of the domain, the digital rights management module causes the transmitter to transmit the digital legacy content from the storage element to the second communication device.

20. A method of operation of a communication device of a domain having one or more communication devices that share a cryptographic key in a domain-based digital rights management environment, comprising:

in response to a user request, the communication device communicating to a domain authority a request to register the communication device into a domain; and

if the communication device is determined to have access to one or more valid cryptographic elements, the communication device receiving over a communications channel a cryptographic key of the domain from the domain authority that links the communication device to the domain.

21. The method of claim 20, further comprising:

the communication device, of a domain having one or more communication devices that share a cryptographic key of the domain, requesting digital content;

in response to the communication device requesting digital content, at least one of the communication device and the domain authority verifying authenticity of the domain; and

upon verification of the authenticity of the domain, the communication device receiving an encrypted form of the requested digital content that is bound to the cryptographic key of the domain to which the communication device is registered.

22. The method of claim 21, further comprising the communication device enforcing usage rules associated with the requested digital content and received in a content package containing the requested digital content.

23. The communication device of claim 22, wherein the content package comprises a binary representation rights table that contains the usage rules.

24. The communication device of claim 23, wherein the binary representation rights table comprises a plurality of sections having predefined tokens.

25. The method of claim 21, further comprising:

a second communication device of the one or more communication devices of the domain requesting the digital content; and

transferring the requested digital content from a storage element to the second communication device.

26. The method of claim 20, wherein removing the communication device from the domain comprises:

in response to the request of the user of the domain to remove the communication device, the communication device transmitting a request that the communication device be removed from the domain; and

in response to the request that the communication device be removed from the domain, the communication device receiving from the domain authority via the secure communications channel a command to remove the cryptographic key of the domain from the communication device.

27. The method of claim 26, further comprising:

upon receiving the command from the domain authority, the communication device removing the cryptographic key of the domain.

28. The method of claim 20, wherein prior to the communication device communicating to a domain authority the request to register the communication device into the domain, further comprising the communication device:

communicating to the domain authority a request to establish the domain, said request having a domain name and a domain password;

communicating to the domain authority via a communications channel a unique identifier of the communication device;

downloading the cryptographic key created by the domain authority;

29. The method of claim 20, further comprising:

In response to a request of the user of the communication device, the communication device requesting digital content that is not available in the domain; and

after authenticity of the domain has been verified, the communication device receiving an encrypted form of the requested digital content that is bound to the cryptographic key of the domain to which the communication device is registered.

30. The method of claim 29, wherein the encrypted form of the requested digital content is contained in a content package having usage rules enforced by the communication device.

31. The communication device of claim 29, wherein the content package comprises a binary representation rights table that contains the usage rules.

32. The communication device of claim 31, wherein the binary representation rights table comprises a plurality of sections having predefined tokens.

33. The method of claim 29, further comprising the communication device storing the encrypted digital content in an open-access storage element.

34. The method of claim 29, further comprising:

the communication device receiving a request from a second communication device of the one or more communication devices of the domain requesting the digital content;

the communication device verifying the authenticity of the second communication device; and

if the authenticity of the second communication device is verified, the communication device transferring the requested digital content from a storage element of the communication device to the second communication device.

35. The method of claim 20, further comprising:

the communication device receiving digital legacy content from a source external to the domain and storing it in a storage element of the communication device; and

in response to a request from a second communication device of the domain, the communication device transmitting the digital legacy content from the storage element to the second communication device.

36. A method for registering devices in a domain having one or more communication devices that share a cryptographic key in a domain-based digital rights management environment, comprising:

a domain authority receiving a request to add a communication device to the domain;

the domain authority determining whether the communication device is legitimate by verifying that the communication device has access to one or more valid cryptographic elements;

if the communication device is determined to be valid, the domain authority transmitting over a communications channel to the communication device a cryptographic key of the domain operable to link the communication device to the domain.

37. The method of claim 36, wherein prior to the domain authority transmitting the cryptographic key to the communication device further comprising:

The domain authority determining that the one or more communication devices of the domain do not exceed a predetermined upper limit.

38. The method of claim 36, further comprising prior to receiving a request to add the communication device to the domain, the domain authority receiving a request to create the domain having a domain name and a domain password;

the domain authority initiating the communications channel with the communication device;

the domain authority determining a unique identification of the communication device;

the domain authority establishing the domain using the unique identification of the communication device, the domain name, and the domain password;

the domain authority creating the cryptographic key of the domain; and

the domain authority providing the cryptographic key for download by the communication device.

39. The method of claim 36, further comprising:

in response to a communication device of the domain requesting digital content, the domain authority verifying authenticity of the domain.

40. The method of claim 36, wherein removing the communication device from the domain comprises the domain authority:

receiving the request to remove the communication device from the domain;

authenticating the communication device; and

upon authenticating the communication device the domain authority transmitting via a secure communications channel to the communication device a command to remove the cryptographic key of the domain from the communication device.

41. The method of claim 36, further comprising the domain authority:

maintaining a log of requests by the communication device to register to or be deleted from one or more domains;

monitoring the log to identify potentially fraudulent activity by the communication device; and

generating a warning message in response to identifying potentially fraudulent activity by the communication device.

42. The method of claim 41, further comprising revoking a public key of the communication device if the communication device is determined to be engaged in fraudulent activity.

43. A domain-based digital rights management system, comprising:

a communication device linked via a first communications link to a domain-based digital rights management environment, comprising:

a processing element;

a receiver, coupled to and controlled by the processing element, operable to receive incoming messages to the communication device;

a transmitter, coupled to and controlled by the processing element, operable to transmit output messages of the communication device; and

a digital rights management module coupled to the processing element that controls operation of the communication device within the domain-based digital rights management system;

a domain authority coupled to the communication device via a second communications link;

wherein the digital rights management module of the communication device in combination with the domain authority are operable to selectively add the communication device to a domain having one or more communication devices that share a cryptographic key and thus permit the communication device to selectively receive and decrypt digital content based upon membership in the domain.

44. A method of limiting access to digital content in a domain-based digital rights management environment, comprising:

a first communication device, of a domain having one or more communication devices that share a cryptographic key of the domain, requesting digital content;

in response to the request from the first communication device, verifying authenticity of the domain; and

upon verifying authenticity of the domain, making the requested digital content accessible to the first communication device by binding an encrypted form of the requested digital content to the cryptographic key of the domain to which the first communication device is registered.

45. The method of claim 44, wherein the encrypted form of the requested digital content is contained in a content package having usage rules enforced by the first communication device.

46. The communication device of claim 45, wherein the content package comprises a binary representation rights table that contains the usage rules.

47. The communication device of claim 46, wherein the binary representation rights table comprises a plurality of sections having predefined tokens.

48. The method of claim 44, wherein prior to the first communication device requesting digital content establishing the domain, said establishing further comprising:

in response to a user request, the first communication device communicating to a domain authority a request to register the first communication device into the domain;

the domain authority determining whether the first communication device is legitimate by verifying that the first communication device has access to one or more valid cryptographic elements; and

the first communication device receiving over a communications link a cryptographic key of the domain from the domain authority that links the first communication device to the domain.

49. The method of claim 44, further comprising:

a second communication device of the one or more communication devices of the domain requesting the digital content; and

transferring the requested digital content from a storage element to the second communication device.

50. The method of claim 44, further comprising:

a second communication device of the one or more communication devices of the domain receiving digital legacy content from a source external to the domain and storing it in a storage element of the second communication device; and

In response to a request from a third communication device of the domain, the second communication device transmitting the digital legacy content from the storage element to the third communication device.

51. The method of claim 44, further comprising removing a second communication device from the domain in response to a request from a user of the domain.

52. The method of claim 51, wherein removing the second communication device from the domain comprises:

in response to the request of the user of the domain to remove the second communication device, the second communication device transmitting a request to the domain authority to remove the second communication device from the domain;

in response to the request that the second communication device be removed from the domain, the domain authority transmitting a command via the secure communications channel to remove the cryptographic key of the domain from the second communication device; and

upon receiving the command from the domain authority, the second communication device removing the cryptographic key of the domain resident on the second communication device.

53. The method of claim 52, wherein the request that the second communication device be removed from the domain is made by the user at a website of the domain authority.